Ющук Ольга Володимирівна,
магістр документознавства та інформаційної діяльності Національного університету „Острозька академія"

ІНФОРМАЦІЙНА БЕЗПЕКА КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ

Розкривається поняття інформаційної безпеки, вказуються основні загрози, з якими найчастіше стикається користувач в Інтернеті. Аналізуються шляхи використання мережі Інтернет в злочинних цілях, актуальність розробки адекватних механізмів протидії злочинним проявам задля забезпечення інформаційної безпеки користувачів мережі Інтернет в державі.

In article the author describes the concept information security, indicates the main threats the user deals with in the Internet. The author analysis the possibilities to use Internet to reach criminal aims, explain the actuality of discovering the adequate mechanisms of counteraction to criminal actions in order to ensure the information security to the Internet user in the in the state.

Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід'ємною складовою яких є інтенсивне використання досягнень сучасних інформаційних технологій. Після вибору Україною шляху до інтеграції в Європу, яка сьогодні активно розбудовує інформаційне суспільство, гостро постала проблема ефективного забезпечення інформаційної безпеки молодої держави.

Бурхливий розвиток інформаційних технологій, призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації (ЗМІ). Інформатизація та комп'ютеризація докорінно змінюють облич-

чя суспільства. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки країни. Метою статті є вивчення сучасного стану інформаційної безпеки, та виявлення основних загроз з якими найчастіше зустрічається користувач в мережі Інтернет.

Останні роки у світі, як ніколи, активно відбувається формування інформаційного суспільства. Інформаційні системи та технології насичують усі сфери сучасного життя, вдосконалюються, розвиваються, стають незамінною складовою існування людини. І, напевне, найважливішим елементом такого поступу є глобальна мережа – Інтернет. Сьогодні Інтернет набуває – значення життєвого простору. Інтернет дозволяє отримувати та розміщувати інформацію, вільно публікувати свої думки, здійснювати групове чи індивідуальне спілкування, обговорення тощо; через Інтернет можливо отримати роботу та платню за неї, здійснити покупку чи перерахувати на певний рахунок гроші, розмістити рекламу, створити поштову скриню, знаходити потрібну інформацію та інше. В багатьох випадках використання Інтернет дозволяє замінити традиційні засоби листування на електронні, які, без сумніву, набагато зручніші та швидші. Сукупність усіх сервісів, що надає мережа Інтернет, дозволяє використовувати їх в якості потужної бази для забезпечення освітніх процесів.

За наявності таких позитивних моментів існує низка проблем, адже протягом останніх років спостерігається стійка тенденція до різкого збільшення загроз з точки зору кількості спроб несанкціонованого втручання в роботу інформаційних та телекомунікаційних систем, та несанкціонованого доступу до інформації, яка в них циркулює, а також появи нових методів та алгоритмів щодо їх здійснення. Таке втручання створює реальну загрозу національному інформаційному простору України та у разі неприйняття необхідних заходів може призвести у найближчому майбутньому, до втрати державою контролю над частиною її інформаційного простору та, відповідно, неможливості забезпечення прав громадян у цій сфері.

У сучасному світі інформація відіграє надзвичайно важливу роль. Кажуть, хто володіє інформацією, той володіє світом. З нею тісно пов'язані численні права і свободи громадян, життєві інтереси суспільства та держави. Тому неповнота, несвоєчасність або неточність інформації може завдати їм суттєвої шкоди [5]. Стан захищеності інтересів громадян, суспільства та держави в інформаційній сфері називають інформаційною безпекою. З іншого боку під інформаційною безпекою слід розуміти такий стан за-

хищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [4].

Інформаційна безпека складається з багатьох компонентів. Вона залежить і від рівня забезпечення свободи слова в державі, і від захищеності громадян від впливу на їх світосприйняття, психічне та фізичне здоров'я таких негативних чинників, як пропаганда жорстокості, насильства, і від

наявності у органів влади достатньої інформації для прийняття відповідних рішень, тощо [5].

В. О. Голубєв розуміє під інформаційною безпекою людини, суспільства, держави такий стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [3]. Виходячи з цієї ідеї, можна зробити висновок, що головним завданням інформаційної безпеки є формування менталітету стійкого прогресивного розвитку. В цьому процесі надзвичайно велика питома вага саме інформаційного впливу як на людину, так і на все те, що відбувається в колективі людей, в суспільстві, у державі.

У сучасному комп'ютерному суспільстві атаки на інформацію стали буденною практикою. Повідомлення про атаки "хакерів" і комп'ютерні злами заповнили всі засоби масової інформації. З масовим впровадженням комп'ютерів у всі сфери діяльності людини об'єм інформації, що зберігається в електронному вигляді, виріс в тисячі разів. І тепер скопіювати за півхвилини і винести носій з файлом, що містить план випуску продукції, набагато простіше, ніж копіювати або переписувати безліч паперів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

Прикладів підміни, "зламу", втручання у конфіденційну інформацію можна навести безліч. Так у банківській сфері Російської Федерації відбувся великий витік інформації. У продажі на чорному ринку з'явилася база даних, яка містить інформацію про три мільйони клієнтів провідних російських банків. База складена з "чорних списків" десяти найбільших банків, які займаються споживчим кредитуванням. У документах є інформація про

ім'я позичальника, його телефон, домашня адреса, місце роботи і причини потрапляння в "чорний список". Компакт-диск з базою даних продають усього за 2 тис. рублів [5].

Варто поглянути на проблеми в галузі комп'ютерних технологій Корпорація IBM Internet Security Systems, яка представила результати дослідження інформаційної безпеки в 2007 р. , опубліковані в звіті 2007 X-Force Security, акцентуючи увагу на зростанні витонченості атак злочинців на веб-браузери користувачів у всьому світі. По повідомленню IBM, кіберзлочинці, атакуючи веб-браузери, які призначені для користувача комп'ютерів, здійснюють розкрадання конфіденційної персональної інформації, що ідентифікує особу користувачів, в небачених раніше масштабах. Результати дослідження IBM свідчать, що витончені атаки з боку кримінального співтовариства все частіше направлені на отримання незаконних прибутків від "експлуатації" вразливостей Веб [6]. Посібники кіберзлочинців надають їм інструментарій для маскування атак на веб-браузери, що допомагає уникнути виявлення таких атак системами інформаційної безпеки. У 2006 р. лише невеликий відсоток атакуючих використовував технології "камуфляжу" (технологія, за якої система захисту комп'ютера від несанкціонованого доступу не може побачити ніяких збоїв при роботі комп'ютера), проте вже протягом першої половини 2007 р. цей показник стрімко виріс до 80% і до кінця року досяг майже 100%. За прогнозами фахівців X-Force, в 2008 р. число атак збільшиться на декілька тисяч [3]. Завдяки такій техніці атак кіберзлочинці можуть проникнути в систему користувача і отримати доступ до особистої інформації, такої як: номери страховок і ідентифікаційних документів, дані кредитних карт і таке інше. Атакуючи корпоративний комп'ютер, зловмисники можуть отримати доступ до важливої комерційної інформації і використовувати заражений комп'ютер, щоб обійти захист брандмауера.

Продовжуючи тему сучасних проблем забезпечення інформаційної безпеки України можна виділити кілька, які найбільш актуальні кожному пересічному громадянину-споживачу інформації (глядачу, читачу тощо). 35% повідомлень української преси стосуються тем насильства, жорстокості, злочинної діяльності тощо. Не краща ситуація і в царині електронних ЗМІ (телебачення і радіо). Подібна інформація ганьбить людську гідність, особливо негативно впливає на психіку дітей та молоді, створює відповідний настрій у суспільстві [1].

Ще одна проблема українського інформаційного простору – засилля іноземної (переважно російської) теле-, радіо-, друкова-

ної продукції. Так, в Україні популярними є такі телерадіокомпанії Російської Федерації, як: НТВ, ОРТ, РТР, ТНТ, "Русское радио", "Европа-Плюс" та інші. За участі Фонду Російської Федерації "200-ліття Пушкіна" створений найбільш рейтинговий (популярний) в Україні телеканал "Інтер". Існує ще один промовистий факт: до каталогу періодичних видань, які щороку пропонуються увазі українським передплатникам, включається у два рази більше видань з Росії, ніж з України [1].

Небезпека такого стану речей полягає у тому, що український інформаційний простір формується багато в чому за рахунок тем та проблем, які нагальні для іноземної держави та висвітлюються з позиції її власних інтересів. А оскільки українські громадяни мають невеликий вибір, особливо з-поміж теле– і радіопрограм, їм просто нав'язують позиції, які далеко не завжди відповідають дійсності та національним інтересам України. Крім того, зарубіжна інформаційна продукція створює серйозну конкуренцію вітчизняним ЗМІ і заважає їх нормальному розвитку. Останні втрачають прибутки не лише від зменшення кількості передплатників, покупців, але й завдяки зменшенню обсягів реклами, розповсюдження якої їм замовляють [5].

У Законі України "Про безпеку користувачів телекомунікацій" чітко зазначено що користувач – це фізична особа, яка користується інформаційною послугою для задоволення своїх споживчих чи ділових потреб, використовуючи кінцеве обладнання, розташоване на території України, але ж як користувач може використовувати ту чи іншу інформацію в Інтернеті для задоволення своїх потреб, якщо його на кожному кроці намагаються обманути? В законі також визначено гарантію прав споживачів, особливо що стосується безпеки інформаційних послуг: постачальник інформаційної послуги повинен вживати відповідних технічних та організаційних заходів для гарантування безпеки своїх послуг, захисту інформації, запобігання несанкціонованого доступу до телекомунікацій відповідно до вимог законодавства про захист інформації в автоматизованих системах. Постачальник несе відповідальність за надання інформаційної послуги, яка містить заборонену до поширення інформацію, відповідно до законодавства [10]. А чи часто постачальник інформації в глобальній мережі Інтернет повідомляє користувача про можливу загрозу витоку його конфіденційної інформації? Напевно що ні. Отже, ми спостерігаємо явне порушення закону. Тому вже сьогодні необхідним є відповідна координація зусиль щодо забезпечення протидії цьому виду правопорушень.

Не менш важливою проблемою забезпечення інформаційної безпеки користувачів є небажання людей вірити в те, що з ними щось може трапитися – до тих пір поки це не трапиться. Насправді неприємності трапляються значно частіше ніж думають більшість користувачів. Незалежно від того яким способом і з якої причини була здійснена атака на комп'ютерну систему, відновлення займе багато часу і сил. Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи. Правові методи – передбачають розробку комплексу нормативно-правових актів і положень, які регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки. Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах. Програмно-технічні методи – це сукупність засобів для: запобігання витоку інформації; виключення можливості несанкціонованого доступу до інформації; запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації; виявлення прикладних пристроїв; виключення перехоплення інформації технічними засобами; використання криптографічних засобів захисту інформації при передачі по каналах зв'язку.

При вивченні проблеми інформаційної безпеки, нами було розроблено ряд корисних порад користувачам мережі Інтернет, які варто знати. Отож для захисту себе від несанкціонованого втручання потрібно знати та використовувати необхідні програми захисту такі як: брандмауери (фаєрволи), та антивірусні програми. При використанні електронної пошти потрібно:

Уважніше відкривати підозрілі листи електронної пошти, або ж не відкривати їх взагалі;

Використовувати фільтр спаму програми електронної пошти;

При запитах в Інтернеті користуватися додатковою електронною поштою;

Не пересилати "ланцюгові" повідомлення електронної пошти. Видаляти їх одразу після надходження.

В мережі Інтернет потрібно бути дуже обачним та закривати сумнівні спливаючі вікна; не допускати того, щоб вас ошукали;

завжди оновлювати операційну систему; робити резервні копії важливих файлів; дотримуватися правил та законів навіть в Інтернеті. Хоча більшість законів було створено до того, як Інтернет набув широкого розповсюдження, дія законів розповсюджується і на Інтернет. Все, що є незаконним у повсякденному житті, є незаконним і в он-лайні; Варто також пам'ятати, що при розміщенні інформації в Інтернеті, втрачається контроль над нею; не рекомендується зберігати особисту інформацію у веб-браузері та інших програмах, з'єднаних із Інтернетом.

Це найголовніші правила, яких так чи інакше варто дотримуватись задля забезпечення захисту конфіденційної інформації, що стосується як користувача особисто, так і інформації для роботи.

Підсумувавши все вище зазначене слід сказати, що на даному етапі розвитку інформаційних технологій, існує загроза забезпечення інформаційної безпеки користувачів мережі Інтернет. Для реалізації цього комплексного завдання державі необхідно відшукати динамічний баланс між свободою слова, забезпеченням права на інформацію, ефективним використанням її як засобу контролю громадянського суспільства за діями влади, обмеженням поширення таємної інформації та підтриманням моральної і духовної стабільності у суспільстві. Знаходження цього балансу дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної і якісної інформації. Це завдання передбачає здійснення гнучкої і активної державної політики у питаннях циркуляції інформації, доступу до неї, діяльності засобів масової інформації, розвитку видавничої справи, освіти і масової культури. Найкраще забезпечити інформаційну безпеку українська держава зможе, якщо створить умови для всебічного розвитку інститутів громадянського суспільства, закладів освіти і культури, засобів масової інформації.

Державна політика має передбачати системну превентивну діяльність органів влади з надання гарантій інформаційної безпеки особі, суспільним групам та суспільству в цілому. Взагалі, доцільно законодавчо визначити інформаційну безпеку України як комплекс системних превентивних заходів із наданням гарантій захисту життєво важливих інтересів особистості, суспільству й державі від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного

суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз. Та не менш важливим є поінформованість користувачів, із загрозами які чекають їх на кожному кроці. Ступінь обізнаності користувачів у сучасній ситуації представлених загроз – запорука якісній роботі, та необхідному захисту, в таких важливих, на сьогоднішній день реаліях.

Список використаних джерел та літератури:

Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД // Національна безпека і оборона. – К. , 2001. – №1. – С. 2-59.

Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах/ В. Гавловський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. , 2000. – №1. – С. 50-53.

Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю / В. О. Голубєв. – Запоріжжя, 2003. – 250 с.

Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання / В. Гурковський // Вісник Української академії державного управління при Президентові України. – К. , 2002. – №3. – С. 27-32.

Калюжний Р. А. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю [Електронний ресурс] / Р. А. Калюжний, В. С. Цимбалюк. – Режим доступу: www. URL: www. crime-research. org. – Заголовок з екрану.

Кузнецов В. Комп'ютерна інформація як предмет крадіжки / В. Кузнецов // Право України. – К. , 1999. – №7. – С. 85-88.

Національна безпека України, 1994-1996рр. : наукова доповідь НІСД / гол. ред. О. Ф. Бєлов. – К. : НІСД, 1997. – С. 124-133.

Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзюбань, В. К. Пархоменко, Д. В. Дмитрієв. – Х. : "Фоліо", 2002. – С. 152-167.

Правове регулювання інформаційної безпеки у сфері підприємницької діяльності / В. Ніколаєв, Г. Остапович, І. Костицька та ін. – К. , 2002. – С. 19-25.

Про безпеку користувачів телекомунікацій: проект закону України від 29 жовтня 1998р. №876/1998 [Електронний ресурс] . – К. , 1998. – Режим доступу: www. URL: http:// gska2. rada. gov. ua/pls/zweb_n/webproc34?id="pf3511=14628